REMARKS

Claims 1-18 were present for examination in the above-identified application. All claims stand rejected under 35 U.S.C. 102(e) as anticipated by U.S. Patent 6,502,135 to Munger et al. Additionally, the Abstract has been objected to as being too lengthy. The Abstract has been shortened by the present amendment to less than 150 words.

Virtual Private Networks (VPN) for establishing communication through a Packet Network such as the internet are known. As described in the present application (and shown by VPN definition 3 of the attached page 813 of Newton's Telecom Dictionary) a source of information such as a user's computer encrypts, compresses, etc. a data payload and transmits it to the internet with the destination address of a security gateway. The packet finds its way through the various modes of the internet and is delivered to the security gateway which is the interface between the internet and a secure network. The gateway is responsible for accessing the payload for use on the secure network by performing necessary VPN protocols to authenticate, decompress, decrypt etc. the payload. (see the attached definition from Newton's Telecom Dictionary, pg 322). Applicants invention, as is stated in all independent claims 1,10 and 15 relates primarily to accessing of the payload at an internet security gateway.

In contrast, the Munger et al. reference relates primarily to the conveyance of packets through the nodes of the internet in such a way that it is difficult for an "eavesdropper" to identify all of the parts of a message and which originating terminal is communicating with which destination terminal. The individual TARP routers of the Munger et al. internet 107 produce at random, many paths for the individual message packets to take between the

originating terminal and the destination terminal. Gaining access to the payload of messages by the TARP terminal 110, which is the gateway of the Munger et al., system is not discussed in detail. For example, column 1, lines 38-45 merely states that encryption keys may be known to the origination and destination terminals so that data security can be maintained. Accordingly, the present inventions and Munger et al., do not even relate to the same aspect of VPN communication.

Applicant's claims have been amended to clarify that the gateway function of gaining access to packet payloads is being provided. This is a substantially different function than randomizing the paths that packets take while traversing the internet. Apparatus claim 1 is limited to the parts and functions of a security gateway to gain access to the payload of a packet. Nothing can be found in Munger et al., suggesting any relevant detail of its gateway or destination terminal. The gateway of claim 1, as amended, includes a plurality of protocol modules each of which processes packets in accordance with a different virtual private network protocol to access the payload of a received packet. The Examiner cites sections of Munger et al., relating to the functions of the TARP routers which comprise the internet 107 of the Munger et al. disclosure. Nothing is disclosed therein about the functions of the TARP routers to gain access to the payload of packets. Instead they perform a clever algorithm to assure randomized transmission of packets through the network.

The security gateway of applicants claim 1 also includes a memory storing information identifying which of the protocol modules is to process each packet and the sequence of their processing to gain access to the payload. No such memory is taught or suggested by Munger et al. The Examiner refers to col 8, lines 58-61 and refers to as a look up terminal to show such a memory. The entire paragraph from col 8, lines 51-67 clearly

indicates that each TARP terminal includes a look up table which is used to identify where packets are to be directed through the network. The table may be updated from time-to-time by connected terminals. This is clearly not a memory in a gateway which identifies which modules and in what sequence process packets to gain access to the payload.

The security gateway of claim 1 as amended also includes a protocol discriminator which in response to the protocol sequence information of the memory passes a received data packet to the appropriate protocol modules to gain access to the payload. Thus, it is clear that the protocol discriminator is different from anything suggested by col 8, lines 1-15 of Munger et al., which merely describes the randomizing algorithm employed by the TARP routers. In view of the foregoing, applicant asserts that claim 1 as amended and claim 2-9 which depend therefrom are allowable as they now stand.

In addition to the above, claim 2 recites that each protocol module of the gateway passes received packets back to the discriminator module upon completion of its processing. The TARP routers of Munger et al., may pass packets on to subsequent TARP routers, but nothing in Munger et al.,teaches or suggests sending them back to a discriminator module. Claim 3 depends from claim 2 and further states that the discriminator module sends the data packets received from one protocol module on to another protocol module. The network of Munger et al., teaches or suggests no such operation.

Claim 10 is a method claim which is similar to claim 1 and is asserted to be allowable for the reasons set forth above concerning claim 1. Claims 11-14 are also asserted to be allowable due to their dependence on claim 10.

Additionally, claim 11 recites that the gateway of claim 10 accumulates the information describing the sequence of protocol

module operations during authentication of the communication. This is different from the address updating described in Munger et al., col 30, lines 28-33 and is undertaken for an entirely different purpose.

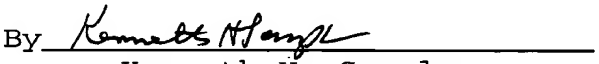
Claim 15 recites a method of operating a security gateway and has been amended to clarify that the operations are being performed to gain access to the payloads of packets. This claim differs from prior claims in that it sets forth a specific method for binding payload access rules and policies to the packets to which the rules and policies are to be applied. This claim recognizes that the originating user has a user identity disclosed in at least one packet and that the packets from that user will be conveyed having an assigned IP address. Initially, a set of rules and policies is stored in the security gateway in a way which associates them with the identify of the user. No such step is taught or is suggested by Munger et al. Next, a packet is received at the security gateway and the IP address assigned to the user is identified and based on the user identity and the IP address, a portion of the rules and policies is bound to the IP address. No step of binding rules and policies which were first stored in association with a user identity is taught or suggested by the reference. In view of the foregoing, claim 15 as amended is not anticipated by the Munger et al. reference. Claims 16-18, are asserted to be allowable due to their dependence on claim 15.

Applicant respectfully asserts that, the rejection of claims 1-18 has been traversed for the reasons discussed above.

The Commissioner is hereby authorized to charge any additional fees which may be required in this application under 37 C.F.R. §§1.16-1.17 during its entire pendency, or credit any overpayment, to Deposit Account No. 06-1135. Should no proper payment be enclosed herewith, as by a check being in the wrong amount, unsigned, post-dated, otherwise improper or informal or even entirely missing, the Commissioner is authorized to charge the unpaid amount to Deposit Account No. 06-1135.

Respectfully requested,

FITCH, EVEN, TABIN & FLANNERY

By 
Kenneth H. Samples
Registration No.: 25,747

Date: 1/12/05

120 South LaSalle Street
Suite 1600
Chicago, Illinois 60603-3406
Telephone: (312) 577-7000
Facsimile: (312) 577-7007

OVER 500,000 SOLD

NEWTON'S TELECOM DICTIONARY

The Authoritative Resource for Telecommunications, Networking, the Internet and Information Technology

MORE THAN 20,000 TERMS DEFINED

18th Updated and Expanded Edition

by Harry Newton

CMPBooks

ing and system applications such as bar code scanners, industrial microwave ovens and wireless monitoring of patient sensors, ISM also is used in many Wireless LANs. As the ISM band is unlicensed, anyone can use it for anything, anywhere in the U.S. Some garage door openers use it-hopefully not the garage door openers at the same hospital that's using it to monitor your pulse rate in the ICU. It's a catch-all, hence the term "garbage band."

Garbage Can What Australians call a garbage can, Americans call a trash can.

Garbage Collection A software program or routine that is used to solve "memory leaks." Garbage collection is the process of searching memory for program segments or data that are no longer active, in order to reclaim that memory space for other computer programs. See also Memory Leak.

Garbage In, Garbage Out GIGO. If the input data is wrong or inaccurate, the output data will be inaccurate or wrong. GIGO is problem with data entered by hand into computer systems. Ask yourself how many times you've received "junk" mail with the wrong spelling of your name? That's called Garbage In, Garbage Out.

Garbitrage Sending garbage from one city to another, usually organized by garbitrageurs on the phone.

GARP 1. Growth At a Reasonable Price. An investment philosophy that focuses on picking stocks that provide growth, but without taking significant risk. The term means different things to different people.

2. Generic Attribute Registration Protocol. An IEEE standard for a generic method by which various devices (e.g., clients, servers, and bridges) can automatically disseminate attribute information across a bridged LAN. GARP is a Layer 2 (i.e., Data Link Layer) protocol used extensively in VLANs (Virtual LANs). A GARP participant consists of a GARP application software component, and a GARP Information Declaration (GID) component which is associated with each port of the bridge. GARP participants in a given application disseminate their attribute information through the use of the GARP Information Propagation (GIP) component. Relying on GARP services is GMRP (GARP Multicast Registration Protocol), which provides a mechanism by which bridges and end stations can automatically and dynamically register their membership in a group with the MAC bridges by which a physical LAN segment attaches to the larger logical LAN. Once the bridges receive that registration information, they propagate it to all other bridges that support extended filtering services. The GARP VLAN Registration Protocol (GVRP) is a GARP application that provides registration services in a VLAN context. See also VLAN.

Gas The word "gas," coined by the chemist J.B. van Helmont, is taken from the word "chaos," which means "unformed" in Greek.

Gas Carbon Used for lightning protection by phone companies. In the telephone's early days lightning often struck telephone lines, electrocuted people or burned their houses down. Early lightning protectors were made of carbon. When hit they took phone out of action and needed to be replaced by a technician. Newer lightning protectors are made with a gas. When hit by lightning they temporarily short, then re-enable the phone line. This invention has greatly reduced the number of bad lines a phone company has after a storm. Despite their name, there is no carbon in them. Gas carbons are the same size and shape as the older carbon protectors so they fit easily into the old slots.

Gas Pressurization A method for preventing water from entering openings in splice closures or cable sheaths by keeping the cables under pressure with dry gas.

Gas Tube A method of protecting phone lines and phone equipment from high voltage caused by lightning strikes. See CARBON BLOCK (another protection technology) for a more detailed explanation. Here is a definition from American Power Conversion Corp. Gas tube is a surge suppression device that clamps a surge voltage to a limited value. Also called a "spark gap", a gas tube is simply two electrodes that are held at a close distance so that high voltages between the electrodes simply arc through the air or other gas within the tube, thereby effectively clamping the voltage. Gas tubes are very slow, but can handle very large surges. The main problem with the use of gas tubes in AC power circuits is that when they clamp the surge they momentarily short out the utility line which usually trips the circuit breaker feeding the circuit which the tube is connected to. In this case the operation of surge clamping leads directly to power interruption. They are well suited to use in data line surge suppression, but have protective clamping voltages that are too high to provide effective protection for most modems or computer ports.

Gaseous Conductors The gases which, when ionized by an electric field, permit the passage of an electric current.

Gate 1. This term is typically used in Automatic Call Distributors, devices used for handling many incoming telephone calls. Gate refers to a telephone trunk or business transaction grouping that may be handled by one group of telephone answerers (called attendants, operators, agents or telemarketers). That one group of telephone answerers is called "the gate." All calls coming into that gate can, theoretically, be handled by any of the telephone answerers. A telephone call is homogeneous throughout the gate. An automatic call distributor may have one gate — all calls coming in can be handled by everyone. Or it may have many gates, each one consisting of the line (or lines) bringing the call in, e.g. Band 5 WATS, New York City foreign exchange line. Or it may have two gates, one for orders and one for service. ACDs with multiple gates will establish rules for moving the calls between the gates, should one gate become overloaded.

2. A circuit on a silicon chip. See Gate Array.

Gate Array A circuit consisting of an array of logic gates aligned on a substrate (a piece of silicon) in a regular pattern.

Gate Assignments Used in context of ACD (Automatic Call Distribution) equipment. Gates are made up of trunks that require similar agent processing. Individual agents can be reassigned from one gate to another gate by the customer via the supervisory control and display station. Also called splits.

Gate D Gateway Daemon. A popular routing software package which supports multiple routing protocols. Developed and maintained by the GateDaemon Consortium at Cornell University.

Gatekeeper In the classic sense of the word, a gatekeeper is someone who is in charge of a gate. His or her job is to identify, control, count, supervise the traffic or flow through it. A network gatekeeper provides the same functions, including terminal and gateway registration, address resolution, bandwidth control, admission control, etc. A gatekeeper is a fancy name for a network administrator.

Gateway 1. A gateway is what it sounds like. It's an entrance and exit into a communications network. That "communications network" may be huge, for example, at the point where AT&T Communications ends and Comsat begins — for taking my satellite call overseas. Gateways may be small — between one LAN and another LAN. Technically, a gateway is an electronic repeater device that intercepts and steers electrical signals from one network to another. Generally, the gateway includes a signal conditioner which filters out unwanted noise and controls characters. In data networks, gateways are typically a node on both two networks that connects two otherwise incompatible networks. For example, PC users on a local area network may need a gateway to gain access to a mainframe computer since the mainframe does not speak the same language (protocols) as the PCs on the LAN. Thus, gateways on data networks often perform code and protocol conversion processes. Gateways also eliminate duplicate wiring by giving all users on the network access to the mainframe without each having a direct, hard-wired connection. Gateways also connect compatible networks owned by different entities, such as X.25 networks linked by X.75 gateways. Gateways are commonly used to connect people on one network, say a token ring network, with those on a long distance network. According to the OSI model, a gateway is a device that provides mapping at all seven layers of the model. A gateway may be used to interface between two incompatible electronic mail systems or for transferring data files from one system to another. Electronic mail systems that sit on local area networks often have gateways into bigger e-mail systems, like Internet or MCI Mail. For example, I might use MCI Mail to send a e-mail to someone's internal LAN e-mail. It might travel from MCI Mail to Internet via a gateway and then from Internet via another gateway to the company's e-mail on its own LAN.

2. A Gateway is an optional element in an H.323 conference. Gateways bridge H.323 conferences to other networks, communications protocols, and multimedia formats. Gateways are not required if connections to other networks or non-H.323 compliant terminals are not needed. Gatekeepers perform two important functions which help maintain the robustness of the network — address translation and bandwidth management. Gatekeepers map LAN aliases to IP addresses and provide address lookups when needed. Gatekeepers also exercise call control functions to limit the number of H.323 connections, and the total bandwidth used by these connections, in an H.323 "zone." A Gatekeeper is not required in an H.323 system-however, if a Gatekeeper is present, terminals must make use of its services. See TAPI 3.0.

Gateway City A city where international calls must be routed. New York, Washington, DC, Miami, New Orleans, and San Francisco are the five gateway cities in the United States.

Gateway Protocol Converter GPC. An application-specific node that connects otherwise incompatible networks or networked devices. Converts data codes and transmission protocols to enable interoperability. Routers are capable of running gateway protocols — we used to call routers "gateways." Contrast to Bridge.

Gateway Server A cor
that use different access protoc
Gating 1. Enabling or disab
nal gets through. If not, the si
2. The process of selecting onl
or between specified amplitud
Gatored To be gatored m
pop-up ads. The term, accordin
that's increasingly bundled wit
Gauge A term for specifyir
lower number in the American
phone conversations further a
cost more and take up more
them in a duct. When buying
cables that will be installed –
tance from the central telephi
you intend to live with your
course, not only specify the c
coax, etc. Gauge is but one
Gauge, Wire The me
important American gauges
Brown & Sharpe, and the St
Gauss The unit of magne
timeter.
Gaussian Beam A b
a fiber core. It can also be
Most people would recogniz
Gaussian Noise G
noise," also known as "wh
occurs when electricity is pc
of electrons in the conduct
quencies involved. Gaussia
German mathematician wh
ory of electricity. Gauss also
the frequency distribution o
Gazillion An extremel
GB Gigabyte. See Gigaby
GbE See Gigabit Etherne
GBH Group Busy Hour.
GBIC Gigabit Interface C
removable optical interfac
Channel traffic. Used as a
Channel Fabric switches.
Gbps Gigabits per secon
GCAC An ATM term. Ge
if a link has potentially er
GCI A TDM (Time Divisi
GCRA An ATM term. E
mance with respect to th
determines whether the
ment the GCRA, or one o
is defined with two paran
GCS Global Communica
GCT Greenwich Civil Ti
GD Graceful Discard.
Discard.
GDDM An SNA defini
used for graphics display
in Macintosh computers.
GDF Group Distributior
GDI Graphics Device I
screens, printers, and ot
tions for drawing lines,

Gateway Server A communications server that provides access between networks that use different access protocols.
Gating 1. Enabling or disabling a signal through applied logic. If it's turned on, the signal gets through. If not, the signal doesn't get through.
2. The process of selecting only those portions of a wave between specified time intervals or between specified amplitude limits.
Gatored To be gatored means that while surfing the Internet, you're bombarded by pop-up ads. The term, according to Wired Magazine, comes from Gator, the ad-feeding app that's increasingly bundled with popular file sharing programs.
Gauge A term for specifying the thickness (diameter) of cables. Thicker cables have a lower number in the American Wire Gauge (AWG) scale. Thicker gauge cables can carry phone conversations further and more clearly than thinner gauge cable. But thicker cables cost more and take up more room, especially when you bundle them together and put them in a duct. When buying a phone system it is good to specify the thickness of the cables that will be installed — especially if some of your extensions will be a great distance from the central telephone switch, if you intend to carry high-speed data on them or you intend to live with your cabling scheme for more than a few months. You should, of course, not only specify the cable's thickness, but also whether it's stranded or solid core, coax, etc. Gauge is but one part of a cable description. See AWG for a fuller explanation.
Gauge, Wire The method of specifying the thickness and size of wire. The two important American gauges are the American Wire Gauge (AWG), previously known as Brown & Sharpe, and the Steel Wire Gauge. See AWG for a fuller explanation.
Gauss The unit of magnetic field intensity in terms of the lines of force per square centimeter.
Gaussian Beam A beam pattern used to approximate the distribution of energy in a fiber core. It can also be used to describe emission patterns from surface-emitting LEDs. Most people would recognize it as the bell curve.
Gaussian Noise Gaussian noise, more correctly, is "average white Gaussian noise," also known as "white noise" and "thermal noise." It is the natural noise which occurs when electricity is passed through a conductor, and is due to the random vibration of electrons in the conductor. Gaussian noise is uniform across the entire range of frequencies involved. Gaussian noise is named after Karl Friedrich Gauss (1777-1855), the German mathematician who is generally recognized as the father of the mathematical theory of electricity. Gauss also invented the "Gaussian Distribution," or "bell curve," which is the frequency distribution of many natural phenomena. See White Noise for more detail.
Gazillion An extremely large, indeterminate amount. See Gigabyte.
GB Gigabyte. See Gigabyte.
GbE See Gigabit Ethernet.
GBH Group Busy Hour.
GBIC Gigabit Interface Connector. The physical connection to Gigabit Ethernet media. A removable optical interface transceiver module designed to carry Gigabit Ethernet or Fibre Channel traffic. Used as a physical-layer transport interface on Gigabit Ethernet and fibre Channel Fabric switches.
Gbps Gigabits per second. Gig is one thousand million bits per second.
GCAC An ATM term. Generic Connection Admission Control: This is a process to determine if a link has potentially enough resources to support a connection.
GCI A TDM (Time Division Multiplexed) bus technology developed by Siemens.
GCRA An ATM term. Generic Cell Rate Algorithm: The GCRA is used to define conformance with respect to the traffic contract of the connection. For each cell arrival the GCRA determines whether the cell conforms to the traffic contract. The UPC function may implement the GCRA, or one or more equivalent algorithms to enforce conformance. The GCRA is defined with two parameters: the Increment (I) and the Limit (L).
GCS Global Communications Service.
GCT Greenwich Civil Time.
GD Graceful Discard. A Frame Term. See Committed Information Rate and Graceful Discard.
GDDM An SNA definition: Graphical Data Display Manager (GDDM) system software used for graphics display and printer devices and performs the same functions as QuickDraw in Macintosh computers.
GDF Group Distribution Frame.
GDI Graphics Device Interface. The part of Windows that allows applications to draw on screens, printers, and other output devices. The GDI provides hundreds of convenient functions for drawing lines, circles, and polygons; rendering fonts; querying devices for their output capabilities; and more.
GDMO Guidelines for the Definition of Managed Objects.
GDOP See Geometric Dilution of Precision
GE Gigabit Ethernet. See Gigabit Ethernet.
GEANT Gigabit European Academic NeTwork. A high-speed optical fiber network proposed to cover 30 European countries at speeds of 2.5 Gbps in 2001 and 100 Gbps by 2004. GEANT is the European version of Internet2. See also Internet2.
Gearhead A geek who particularly loves new hardware. See Geek.
GEDCOM GEnealogical Data COMmunication. GEDCOM is the accepted Genealogical Data Exchange format that allows users of different genealogy programs to exchange data. It was first developed by the Mormon Family History Library in conjunction with the PAF (Personal Ancestry File program). PAF may have been the basis of many of the commercial and shareware programs available today. Genealogy research via the Internet is pursued by millions of people. The major sites are www.ROOTSWEB.com, which supposedly has 50 million hits a month. There is also www.JewishGen.org, which has many special interest groups for various regions (e.g GerSig for Germany). Major commercial sites include www.Ancestry.com, which seems to be buying up many of the earlier programs and companies.
Geek A computer enthusiast who doesn't have a life beyond computers and the Internet. Also called a Techno-Geek. Coined in the early 1940s, a geek was a carnival performer usually billed as a wild man whose act often consisted of biting the heads off live chickens or snakes. "Geek" has its roots in the Greek "geck," meaning "fool." See also Geek Gab and Geekspeak.
Geek Gab "Variety" is a weekly magazine that covers the Hollywood entertainment business. It coined the word "geek gab," which it refers to as the proliferation of Web sites claiming to put forward the latest hot news on films, studios and networks. The "news," however, is often unsubstantiated rumor, can be vicious and can destroy a film.
Geek Testosterone When Microsoft turned over internal company materials to the court in Washington that was hearing its anti-trust case, several people believed that they revealed a company running on "geek testosterone." A geek is a computer enthusiast who doesn't have a life beyond computers. Testosterone is the sex hormone, C19H2802, secreted by the testes, that stimulates the development of male sex organs, secondary sexual traits, and sperm.
Geekosphere A definition courtesy Wired Magazine: The area surrounding one's computer where trinkets, personal mementos, toys and "monitor pets" are displayed. A place where computer geeks show their colors.
Geekspeak Geekspeak is the language geeks speak. A geek is a computer enthusiast who doesn't have a life beyond computers and the Internet.
Gender Connectors, plugs and receptacles are assigned a gender to describe their physical type. Ones with pins are male, and those with holes into which the male pins slide are female. See GENDER BENDER.
Gender Bender A device which changes the gender of a connector, plug or receptacle. A gender bender is typically a small plug with all male pins on one side and all male pins on the other. By plugging a female connector into one side of a gender bender, you've effectively changed the female gender of the cable to male. Alternatively, a gender bender could be female on either side. But a gender bender must be the same on both sides.
Gender Changer Another name for a gender bender. See Gender Bender.
Genderless Connector Also called data connector or hermaphroditic connector. Invented by IBM. The connector doesn't require male and female plugs to make a connection. It was designed for token-ring applications. It was too big and clunky for my taste.
General Availability How a product gets to market varies from one company to another. But typically, along the way, there's something called an alpha — the first version of hardware or software. It typically has so many bugs you only let your employees play with it. A beta is the next version. It's a pre-release version and selected customers (and the press) become your guinea pigs. They give you feedback. After beta, and when the bugs are removed and the features have been fine-honed, comes "general availability." That's when the product is finally available for buying by the general public.
General Call The letters CQ in the international code and used as a general inquiry call.
General Packet Radio Service GPRS. General Packet Radio Service is the data service enhancement for GSM, the European standard digital cellular service. GPRS, a packet-switched service which will support the X.25 and TCP/IP packet protocols, is widely expected to be the next major step forward in the evolution of GSM technology. GPRS, an important component in the GSM evolution entitled GSM+, enables high-speed mobile

haps of voice mail, audio mail, e-mail, and video mail. See also LDAP, MIME, SMTP, VPIM Work Group and www.ema.org/vpimdir/index.htm

VPIM Work Group The goals of the Voice Profile for Internet Mail Work Group include establishing an internationally accepted standard profile of ESMTP/MIME to allow the interexchange of voice and fax messages between voice messaging systems; ensuring that this profile also allows interexchange with non-voice messaging MIME compatible email systems, establishing a directory service to support lookup of the routable address, and establishing a defined mapping specification with other voice messaging. The Group hosted a concept demo at EMA'96, a product demonstration at EMA'97, an info booth at CT Expo '98, and at the Fall 98 VMA Meeting in Athens. VPIM vendors are currently testing products for compatibility with the VPIM specification. The VPIM Specification, version 2 has been approved by the IETF as a Proposed Standard. After a long wait for its references to be published, VPIM v2 was published as RFC 2421 in September 1998. See also VPIM.

VPL An ATM term. Virtual Path Link is a means of unidirectional transport of ATM cells between the point where a VPI value is assigned and the point where that value is translated or removed.

VPN Virtual Private Network. There are several definitions for VPN, and we'll go through them in some detail. But first, we need to explain the overall concept. A VPN is not a private network, but is virtually so. That is to say that it exhibits at least some of the characteristics of a private network, even though it uses the resources of a public switched network. True private networks absolutely guarantee access to network resources, and security is perfect — after all, the network is a private one, comprising dedicated leased lines. Those lines (or, more commonly today, the equivalent bandwidth) have been taken out of shared public use and dedicated to the private use of an end user organization on the basis of a lease arrangement. Those dedicated leased lines often go through various switching centers (e.g., COs or POPs), but go around, rather than through, the switches. As far as the private network is concerned, it's a wire center, rather than a switching center. The dedicated leased lines most commonly are T-carrier or even SONET in nature, directly interconnect two or more end user sites, and can be used for any purposes the end user desires. The end user can run any higher-layer protocol it chooses — after all, it's a private network. Sounds great, doesn't it? Sure, it does, but the costs are high, and the complexities of designing and implementing such a network can be way out of proportion to the benefits. Virtual Private Networks don't exhibit exactly the same characteristics and, therefore, don't perform as well as true private networks, but can come pretty close...and at much lower cost. For example, a VPN might offer priority access to bandwidth and other network resources, whereas a true private network offers guaranteed access at all times. A VPN might offer relatively tight security mechanisms, whereas a private network is totally secure. Now, let's examine the specific definitions.

1. The first VPN was developed for voice networking, but subsequently was developed for use in data networking, as well. Also known in AT&T terminology as a Software-Defined Network (SDN), these original VPNs remain in wide use on both a domestic and an international basis. Currently, they largely are used in support of voice, as Frame Relay and other packet network technologies have proved to be more effective in support of data applications. They are a public service offered by IXCs (IntereXchange Carriers) and making use of the circuit-switched PSTN (Public Switched Telephone Network). Originally known as Switched 56, the current usage of the term "VPN" distinguishes data services offered by AT&T, MCI (now Worldcom) and Sprint from Switched 56/64 Kbps services offered by the LECs (local phone companies). Although the specifics vary by IXC, VPNs offer bandwidth options of 56/64 Kbps, increments of 56/64 Kbps, 384 Kbps and 1.544 Mbps (T-1). The last two options are designed with videoconferencing in mind. VPNs provide transmission characteristics and services similar to those of private lines, including network testing, priority access, and security. Access to a circuit-switched VPN is provided over T-carrier (e.g., T-1 or Fractional T-1) local loops, which are full-duplex, four wire, digital circuits. As VPN services are dial-up services provided over the PSTN, they offer the same inherent any-to-any connectivity provided for voice calls, with the added feature of security through a Closed User Group (CUG). In other words, any location on your VPN can dial any other location on your VPN, but can't dial any number outside the CUG and can't be dialed by any number outside the CUG. VPNs also offer the advantage of the high level of PSTN redundancy, which translates into a high level of network resiliency. This network resiliency compares favorably to private, leased-line networks, which are highly susceptible to catastrophic failure. In fact, VPNs often are deployed as a backup to leased-line networks. VPNs also are extremely effective in support of enterprise data networking in organizations with large numbers of small sites. Small locations with relatively modest communications requirements often cannot be cost-effectively connected to long-haul, leased-line networks. VPNs offer the advantages of flexibility and scalability, as sites can be added or deleted relatively easily, with costs maintaining a fairly reasonable relationship to enterprise network functionality. The processes of network configuration (design) and reconfiguration are greatly simplified as compared to a leased-line network. Provisioning time is also greatly reduced, thanks to the flexibility of the circuit-switched network core — the only dedicated portion of the VPN is the local loop, which is always dedicated, regardless of the network service accessed. Compared to a private network, the greatest disadvantage of VPNs is that all calls are priced based on a usage-sensitive algorithm much like that of a typical call over the PSTN. In other words, costs are calculated by duration and time of day, with prime-time calls being priced at a premium. Day-of-week and other special discounts also apply. Some carriers also consider distance in the pricing of VPN calls. Note, however, that the usage-sensitive costs of a VPN typically are a lot less than the cost-per-minute of a normal dial-up call over the PSTN, sensitive to factors including the number of sites connected, usage volume commitments, and contract length. Purely from a cost standpoint, leased-lines are preferred for networking large sites with intensive communications needs. Leased line networks also can support not only data and video transmission, but also voice, thereby offering the advantage of integration of all communications needs over a single network. Access to a VPN POP (Point of Presence) can be gained directly from the IXC (Inter-eXchange Carrier), from a CAP (Competitive Access Provider), or from the LEC (Local Exchange Carrier). Appropriate access technologies include leased lines, Switched 56/64, and ISDN. See also Switched 56 and Private Line.

2. The second definition of VPN is a fairly generic one, referring to a packet data network service offering with some of the characteristics of a private network. Any packet data network can be used as the foundation for such a VPN, including X.25, TCP/IP, Frame Relay, and ATM networks. Each of these foundation networks is very different in terms of specifics, but they all are highly shared in terms of their basic nature. In order to provide services that emulate, or at least approximate, a private network over a highly shared network core, it is necessary to provide some additional features and mechanisms. One such feature is priority access to bandwidth, which can be accomplished through a variety of mechanisms which variously are intrinsic to the fundamental packet protocol (e.g., ATM) or through supplemental protocols (e.g., MPLS, or MultiProtocol Label Switching, which often is used in Frame Relay and TCP/IP networks). Security is a critical feature, which variously can be imposed through mechanisms such as a Closed User Group (e.g., Frame Relay) or tunneling (e.g., TCP/IP).

3. In contemporary usage, VPN most commonly refers to an IP (Internet Protocol) VPN running over the public Internet. While the ubiquitous nature of the Internet is a huge advantage for data networking, the Internet is inherently both insecure and subject to variable levels of congestion. In order to create a VPN over the Internet, security issues are mitigated through the use of a combination of authentication, encryption, and tunneling. Authentication is a means of access control the confirms the identity of users through password protection or intelligent tokens, thereby reducing the possibility that unauthorized users might gain access to privileged internal computing or network resources. Authentication commonly is the responsibility of an access server running the RADIUS (Remote Access Dial-In User Service) protocol, connected to an access router with embedded firewall software. Encryption is the process of encoding, or scrambling, of the data payload prior to transmission in order to secure it; the decryption process depends on the receiver's possession of the correct key to unlock the safety mechanism. The key is known only to the transmitting and receiving devices. Tunneling is the process of encapsulating the encrypted payload in an IP packet for secure transmission. Tunneling protocols include SOCKv5, PPTP (Point-to-Point Tunneling Protocol), L2TP (Layer 2 Tunneling Protocol), and IPSec (IP Security).

The applications scenarios for IP VPNs include remote access, intranets, and extranets. Remote access VPNs are highly effective in support of telecommuters, mobile workers, and virtual employees. Intranets are used to link branch, regional, and corporate offices. Extranets link vendors, affiliates, distributors, agents, affiliates, and strategic partners into the main corporate office, with the level of access afforded being sensitive to the level of privilege indicated by a combination of password and user ID, as properly authenticated. This definition is courtesy of Ray Horak's excellent book, "Communications Systems and Networks." See also Authentication, Encryption, Extranet, Firewall, Internet, Intranet, and Tunneling.

VPOTS Very Plain Old Telephone Service. No automated switching.

VPT Virtual Private Trunking. VPT - (as it pertains to VPN) - appears as a Frame Relay or ATM service to the enterprise, but uses VPN technology to deliver high-availability services, while enabling service providers to fully optimize trunk bandwidth. See VPN.

VPU 1. Virtual Physical Unit.